

The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

DATE(S) ISSUED:

05/14/2013

SUBJECT:

Adobe ColdFusion Could Allow for Remote Code Execution (APSB13-13)

OVERVIEW:

A vulnerability has been discovered in Adobe ColdFusion which could allow for unauthorized remote code execution. Adobe ColdFusion is an application server that enables rapid development, deployment, and maintenance of web applications. Successful exploitation of this vulnerability could result in an attacker gaining the same privileges as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

SYSTEMS AFFECTED:

- Adobe ColdFusion 10
- Adobe ColdFusion 9.0.2
- Adobe ColdFusion 9.0.1
- Adobe ColdFusion 9.0

RISK:

Government:

- Large and medium government entities: **High**
- Small government entities: **High**

Businesses:

- Large and medium business entities: **High**
- Small business entities: **High**

Home users: Low

DESCRIPTION:

Adobe ColdFusion is prone to a vulnerability that allows for unauthorized remote code execution. Successful exploitation could result in an attacker gaining the same privileges as the logged on user. Depending on the privileges associated with the user, an attacker could then

install programs; view, change, or delete data; or create new accounts with full user rights. Failed exploit attempts will likely cause denial-of-service conditions.

Adobe has released a hotfix that addresses this vulnerability. Instructions to update this application can be found at the following link:

<http://helpx.adobe.com/coldfusion/kb/coldfusion-security-hotfix-apsb13-13.html>

RECOMMENDATIONS:

The following actions should be taken:

- Update Adobe ColdFusion on vulnerable systems using the instructions provided by Adobe <http://helpx.adobe.com/coldfusion/kb/coldfusion-security-hotfix-apsb13-13.html>
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
- Refer Adobe's to publically available ColdFusion 9 and Coldfusion 10 Lockdown guides.

REFERENCES:

Adobe:

<http://www.adobe.com/support/security/bulletins/apsb13-13.html>

CVE:

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-1389>